Lesson 1:
Introduction to the Public Key Infrastructure
Lesson Introduction

Lesson 1: Introduction to the Public Key Infrastructure

Learning Objectives:

a) To gain a basic understanding of the:
   - security requirements addressed by using public key encryption and digital signature
   - roles and responsibilities in the PKI process
   - process to create a PKI user account
   - process to generate a public-private key pair and request a certificate
   - process to use a public or private key.

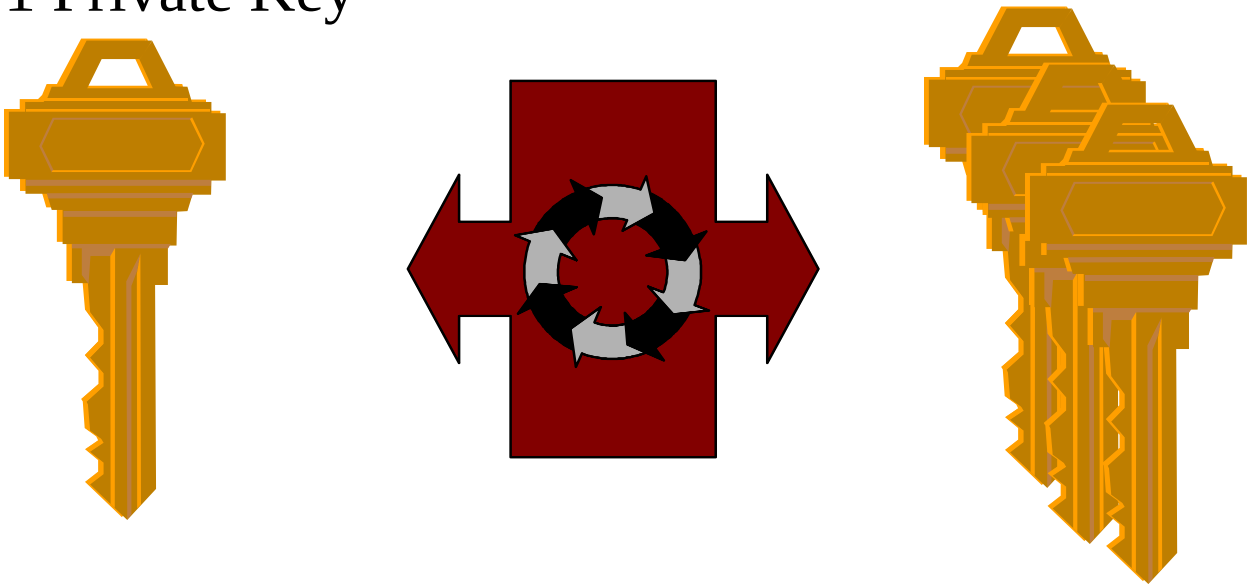
Topic: Security Requirements

Authentication	Assures that a person or system is exactly who or what they claim to be.
Access Control	Provides access to authorized users while denying access to unauthorized users.
Data Integrity	Protects against unauthorized changes in data whether they are intentional or accidental.
Confidentiality	Protects against the disclosure of information to unauthorized users. Encryption is typically used to assure confidentiality when information is transmitted over networks.
Non-Repudiation	Protects against a person denying later that a communication or transaction took place as recorded.
Auditing	Monitors intentional or unintentional misuse of security features.
Availability	Protects against loss of system operation as a result of malicious code, request flooding and penetration attempts

Topic: Security Solutions

Authentication	**Public Key** (Digital Signature) Basic User ID/Password Biometics One-Time Password
Access Control	Discretionary Access Control Firewall Filter Router Single Sign-On Plant Control Authentication Server Proxy Mandatory Access Control Kerberos
Data Integrity	Data Base Referential Integrity Simple Checksum **Public Key** (Digital Signature)
Confidentiality	Database Encryption **Public Key** (encryption) Virtual Private Network
Non-Repudiation	**Public Key** (Digital Signature)
Auditing	Server Client Passive Network Monitoring File Review
Availability	Network Conrol Vulnerability Assessment Virus/Malicious Code Detection

Topic: Key Pairs



User 1 Private Key

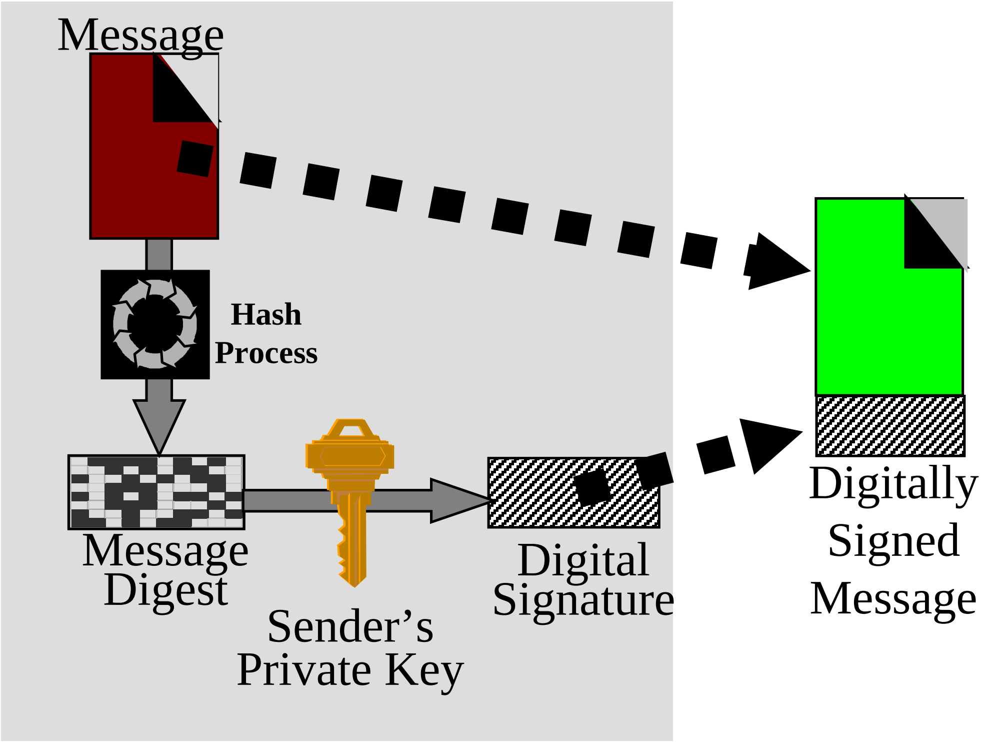
User 1 Public Key(s)

Public key technology is based on key-pairs. User 1 can use their private key to decrypt data encrypted using User 1’s public key and vice versa.
There can be multiple copies of User 1 public keys, but only one copy of the private key, which is held by User 1.

Topic: Using Keys

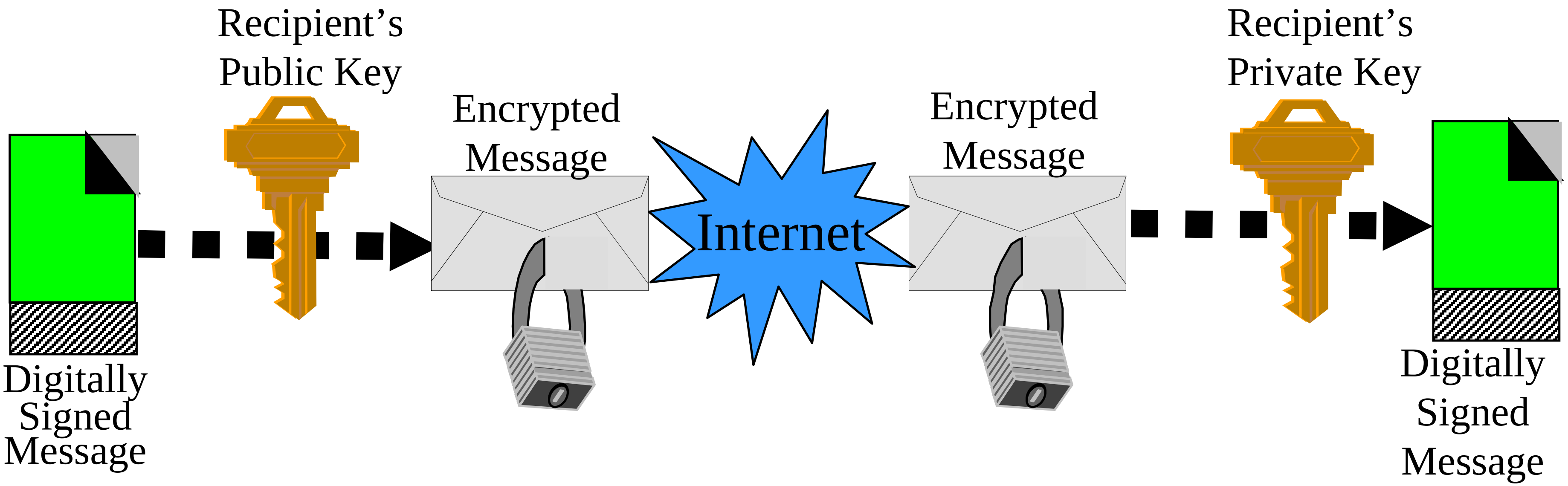
- Keys are used to digitally sign a message and validate this digital signature. A message can be a text or multimedia document.
- Keys are also used to encrypt and decrypt the message.
- A public key can enable access to data encrypted by a corresponding private key. A private key can enable access to data encrypted by a corresponding public key.
- A public key cannot enable access data encrypted by the same public key. A private key cannot enable access to data encrypted by the same private key.
- A user (User 1) retains a private key that he or she uses to send and receive messages. Copies of User 1’s public key are made available via the directory server. Other users who need to verify that User 1 has sent a message, and to encrypt messages intended only for User 1, can access User 1’s public key on the directory server.

Topic: Non-Repudiation



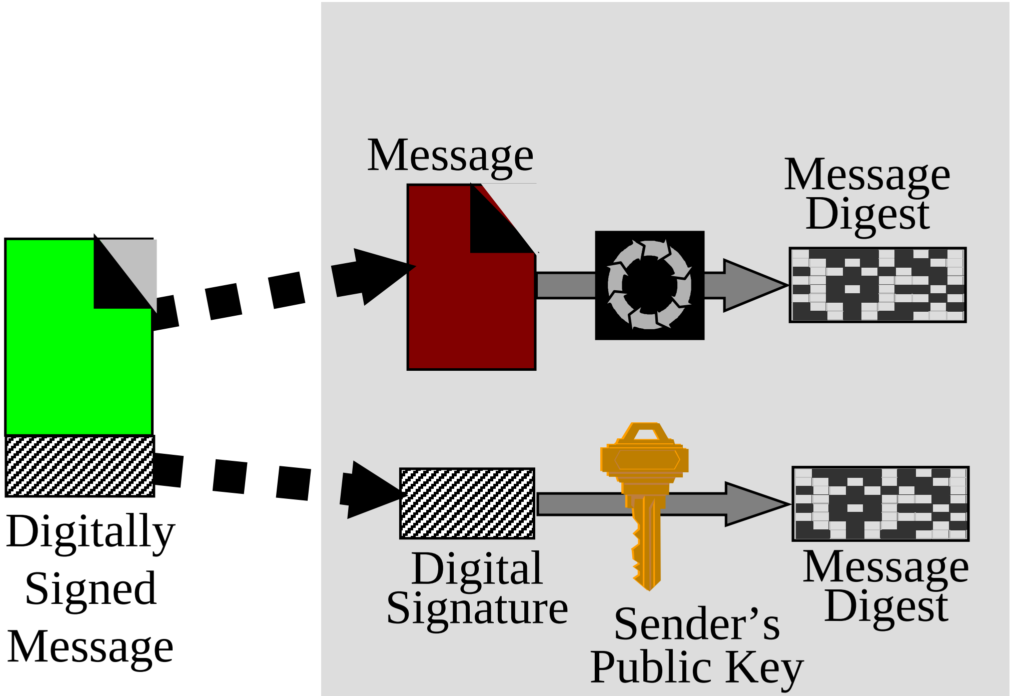
The hashing algorithm creates a message digest based on the contents of the message. The message is then encrypted using the sender's private key and appended to the original message.

Topic: Confidentiality



The digitally signed message can be encrypted using the recipient's readily available public key. This encrypted message is then transmitted via the Internet. Once the encrypted message arrives, the recipient will unencrypt it using his or her own private key.

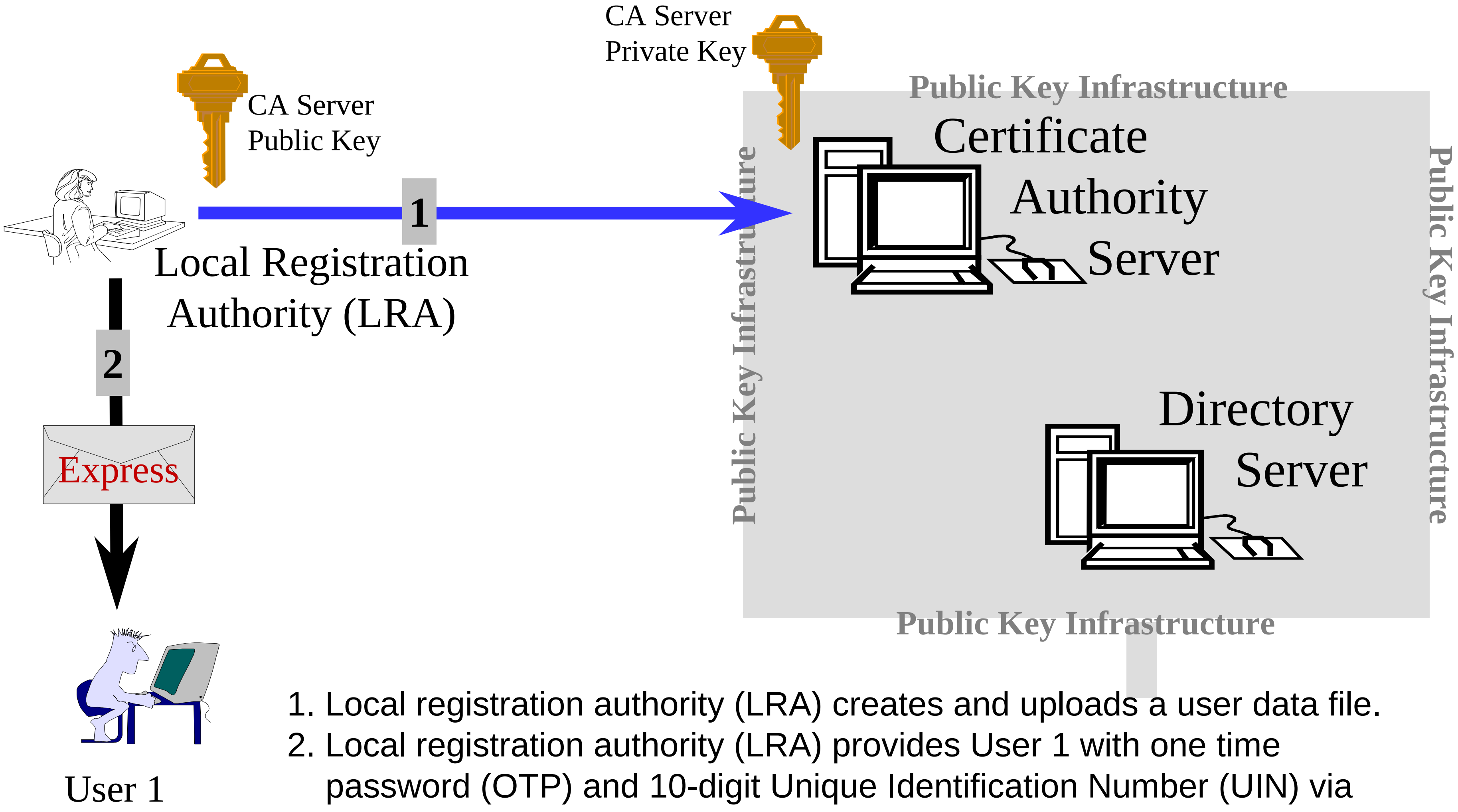
Topic: Data Integrity



To prove that the received message has not been tampered with during transmission, the recipient does the following:

1. Using the same hashing algorithm, creates a message digest of the file as received.
2. Using the sender's public key, decrypts the digital signature to view the original message digest.
3. Compares the two digests to ensure that they are the same.

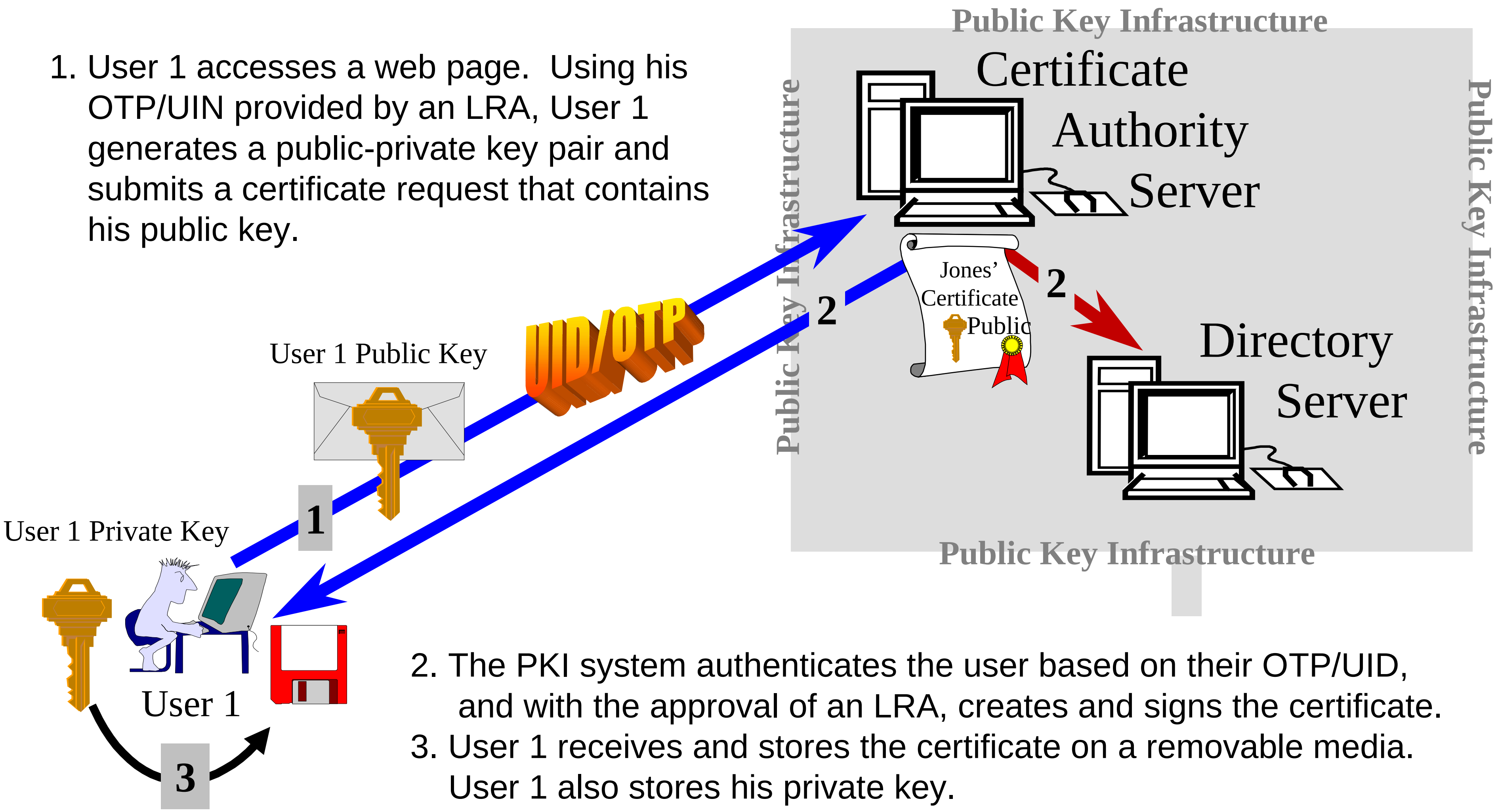
Topic: User Registration



1. Local registration authority (LRA) creates and uploads a user data file.
2. Local registration authority (LRA) provides User 1 with one time password (OTP) and 10-digit Unique Identification Number (UIN) via express mail.

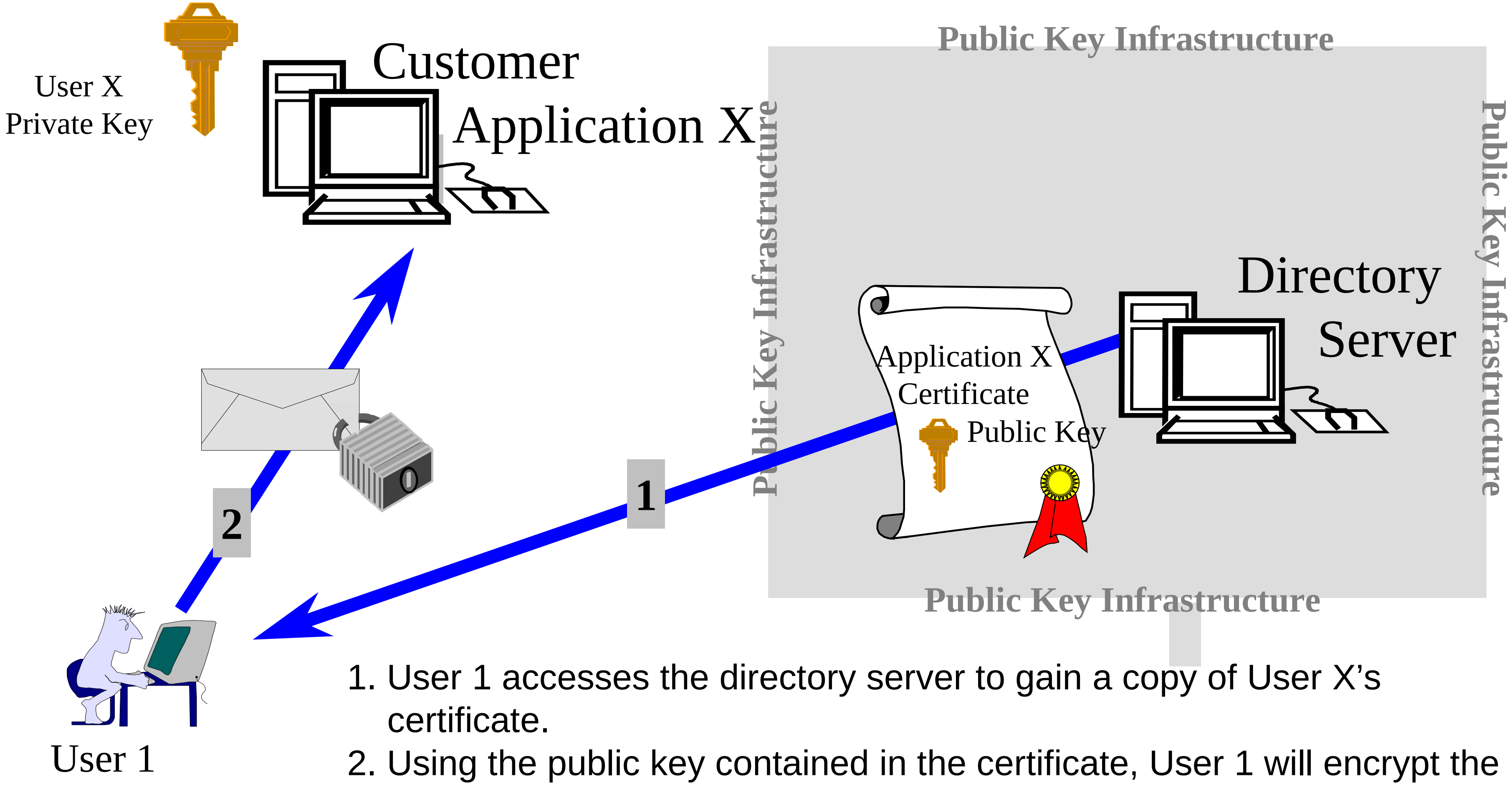
Topic: Generating Key Pairs and Certificates

1. User 1 accesses a web page. Using his OTP/UIN provided by an LRA, User 1 generates a public-private key pair and submits a certificate request that contains his public key.


Public Key Infrastructure
Certificate Authority Server
Directory Server
Public Key Infrastructure
Public Key Infrastructure
Public Key Infrastructure
Jones' Certificate
Public
2
2
UID/OTP
User 1 Public Key
1
User 1 Private Key
User 1
3

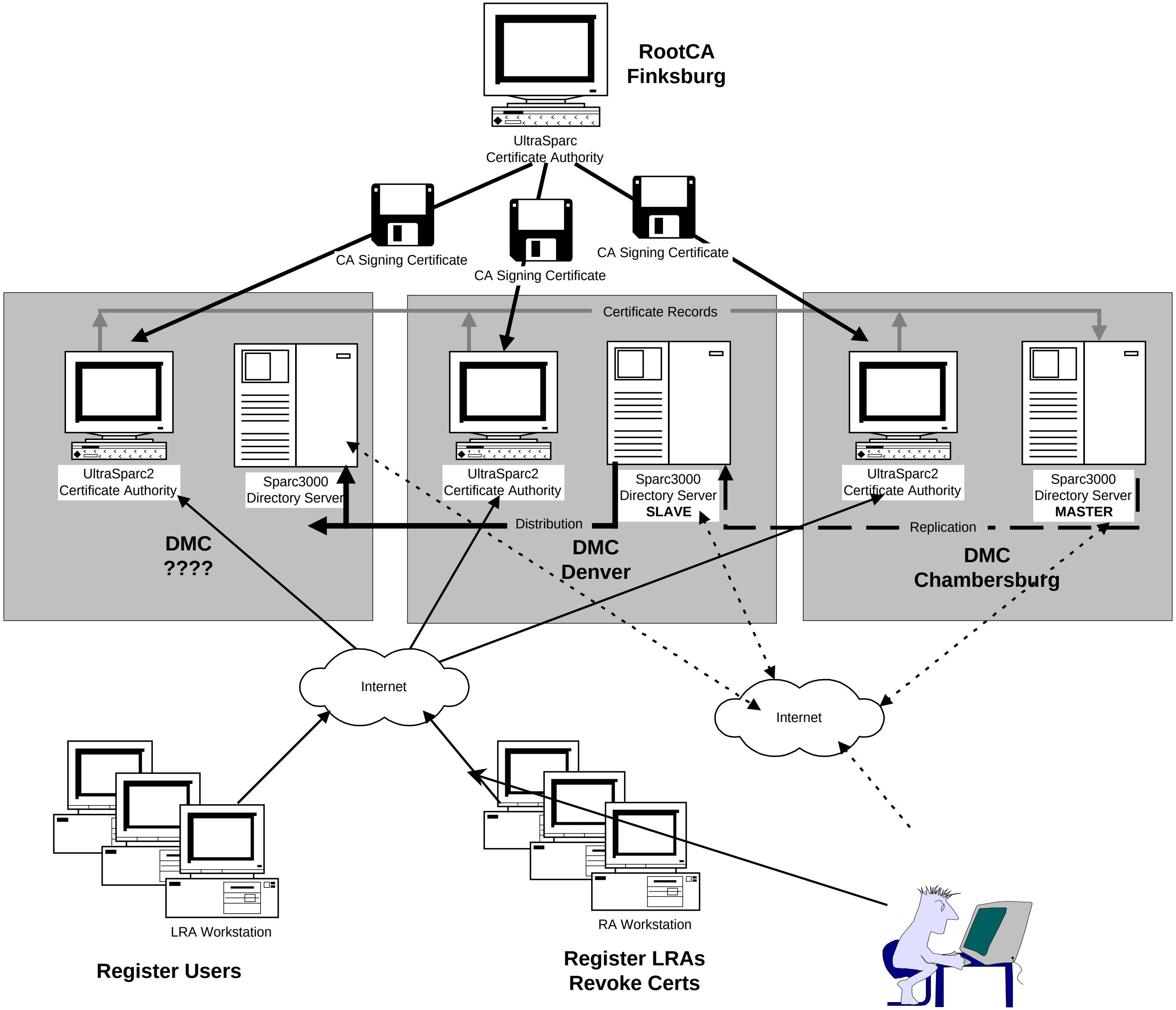
2. The PKI system authenticates the user based on their OTP/UID, and with the approval of an LRA, creates and signs the certificate.
3. User 1 receives and stores the certificate on a removable media. User 1 also stores his private key.

Topic: Accessing Public Keys


User X
Private Key
Customer
Application X
Public Key Infrastructure
Public Key Infrastructure
Public Key Infrastructure
Public Key Infrastructure
Directory
Server
Application X
Certificate
Public Key
1
2
User 1

1. User 1 accesses the directory server to gain a copy of User X’s certificate.
2. Using the public key contained in the certificate, User 1 will encrypt the message to ensure confidentiality during transmission.
3. Once received, the message is decrypted using User X’s private key.

Topic: DoD PKI Architecture



Lesson Summary

This lesson has presented an introduction to:

- Security services provided by public/private keys
- Roles and responsibilities in the PKI process
- Process to generate a PKI user account
- Process to generate a public/private key pair and request a certificate
- Process to use a public/private key.